KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, D.C. 20007-5108

(202) 342-8400

NEW YORK, NY
TYSONS CORNER, VA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

FACSIMILE
(202) 342-8451
www.kelleydrye.com

JOHN J. HEITMANN
DIRECT LINE: (202) 342-8544
EMAIL: jheitmann@kelleydrye.com

November 7, 2006

VIA ECFS

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of Ex Parte Presentation, CC Docket No. 96-115, RM-11277

Dear Ms. Dortch:

XO Communications ("XO"), through its attorneys, respectfully submits this notice of *ex parte* presentation. On November 6, 2006, Lisa Youngers and C.M. Tokë Vandervoort from XO Communications and the undersigned, counsel to XO, met with Michelle Carey, Senior Legal Advisor to Chairman Martin to discuss the Notice of Proposed Rulemaking in the above-referenced proceeding.

During the meeting, XO distributed the attached presentation, which summarizes the scope of the meeting; the content thereof is and XO's oral remarks were consistent with the comments and replies XO previously has submitted in this proceeding. In particular, XO discussed its current security and authentication policies, which are described briefly herein. XO explained that, to the best of its knowledge, those procedures have been sufficient to prevent unauthorized access to account information. XO also urged the Commission not to adopt a rule that would require carriers to implement customer-set passwords, and argued that if the Commission were to adopt some form of customer-set password requirement, then it should limit the requirement so that it applies only to residential customers. To this end, XO proposed an exclusion from any password requirement for business customers.

1. XO's Authentication/Verification Procedures

XO has implemented a multi-tiered process to authenticate a business customer caller's identity prior to releasing customer information.[1] As part of this process, upon becoming an XO customer, each business customer selects a "master account administrator" who has controlling responsibility for and serves as the primary interface on the account. The master account administrator also may choose to designate "sub-administrators" as appropriate for that account. The master account administrator authorizes and thereby limits the type of information (*e.g.*, billing information, trouble tickets, etc.) that each sub-administrator may access. Sub-administrators who have been granted limited account information access are granted access only to information within the scope of their authorized access.

A customer request for information to the XO business customer care call center triggers a multi-step authentication process that involves verification of the business account holder, the caller's identity and scope of authority to access account information, and other account information known only to the customer account. Critically, the XO authentication process includes verification of at least two data points known only to the customer account holder. One of these data points is relatively static while the other is relatively dynamic, so that depending on the account profile, there may be as many as twenty different challenge questions from which an XO business customer care representative may select as part of the authentication of a business customer caller. The use of particular challenge questions varies. The effectiveness of challenge questions in particular is in part due to the variety of questions and the requirement for accurate answers in response.

If the caller successfully provides the required information necessary to authenticate the business customer, the caller and the request being made, then the call continues. If not, XO will refuse the caller's request for account information. For example, if the caller requests billing information, but only has authority to access information pertaining to trouble tickets, then XO will reject the request and instruct that caller that the appropriate authorized sub-administrator or the master administrator must make the request. In XO's experience, this verification process has proven to be extremely robust and has been met with great customer satisfaction.

---

[1] XO serves business customers. The authentication procedures described herein are used for XO's non-web-based business customer care call center. Authentication procedures differ for XO's web-based business customer care interface, and include authentication practices appropriate for Internet commerce.

2. Customer-Set Passwords

XO also urged the Commission not to adopt a rule that would require business carriers to implement customer-set passwords, mandatory or optional. In support of its position, XO noted that there is no evidence that passwords are especially effective when used for live customer-care calls or that passwords are more effective than the multi-tiered authentication procedures already in place at XO and other carriers serving the business market. Indeed, XO indicated that the imposition of any password requirement could reduce the effectiveness of its authentication practices already in place and which have a history of working satisfactorily. XO also noted that the implementation of passwords for non-web-based customer care would be unduly burdensome and costly – especially in the context of business customers.

Although XO does not support any requirement for passwords, XO emphasized that, if the Commission were to adopt a requirement that carriers make available customer-set passwords, then it must limit the requirement so that it applies only to residential customers, as the concerns raised regarding pretexting do not appear to have arisen in the business customer market segment. In support of its position, XO also indicated that passwords are particularly unworkable in the business customer context. This is largely because business customers often have multiple authorized administrators on a single account[2] which in turn exposes passwords to multiple points of potential compromise. In the business customer context, passwords are highly dependent upon the security culture of the particular business customer. Multiple points of access, lax customer password protocols, and potential compromise of passwords increase significantly the burdens associated with the implementation and use of passwords in the business customer setting. Moreover, these complications are likely to interfere with the customer's legitimate requests to obtain account information.

To facilitate definition of the distinction between a residential customer and a business customer in this proceeding so that business customers can be excluded from any password requirement the Commission may elect to adopt, XO proposed that the Commission exclude the following categories of calls from any password requirement:

- Calls pertaining to accounts that have a designated account administrator/manager; and

- Calls made into a business customer care call center.

---

[2] The number, identity and authorization level of administrators on a given business customer account is, by necessity, determined by the customer, and would vary depending on the type of account. For example, a nationwide account customer might designate an account sub-administrator at locations in every state, while designating additional account sub-administrators for handling trouble tickets.

Inquiries on accounts that have a designated account administrator or calls made into a business customer care call center signify that the caller is a non-residential customer.

In sum, multi-tiered authentication as described above represents a proven means of protecting business customer information in a way that is consistent with the Commission's goals of protecting the privacy of customer information. Additionally, as discussed passwords are unworkable in the business context and have the potential to diminish a prudent carrier's already robust authentication practices. Accordingly, adopting a distinction between the business and residential market and excluding the former for purposes of any password requirement also will further the Commission's goals of protecting the privacy of customer information.

Please contact us if you have any questions regarding this filing.

Respectfully submitted,

Jennifer Kashatus

John J. Heitmann
Jennifer M. Kashatus

cc: Michelle Carey (via email)

XO Communications

Ex Parte Presentation – CC Docket No. 96-115, RM-11277

November 6, 2006

Summary

- There is no need to modify the FCC's existing CPNI rules – the FCC's current rules are sufficient to safeguard CPNI
- The FCC should not adopt any of EPIC's proposals
- The FCC also should not modify its rules pertaining to joint venture partners and independent contractors
- XO supports the adoption of a safe harbor

There is No Need to Modify the FCC's Current CPNI Rules

- Comments in this proceeding demonstrate an overwhelming carrier commitment to consumer privacy
- Comments in this proceeding also demonstrate that the risk to customer privacy is due to pretexting or other unlawful practices

The FCC Should Not Adopt Any of EPIC's Proposals

- Adoption of EPIC's proposals would cause carriers to incur significant costs without addressing the underlying problem: pretexting
- Customer-set passwords
  - Passwords are unworkable for business customers because the implementation of customer-set passwords on accounts with multiple administrators would be extremely costly and difficult to administer
  - Consumers do not want passwords
- Audit trails
  - FCC already has rejected the use of audit trails and there is no reason to revisit that decision
  - It would be extremely costly and burdensome for carriers to change or modify their databases to be able to implement audit trails

The FCC Should Not Adopt Any of EPIC's Proposals (cont.)

- Encryption
  - Unnecessary if a carrier maintains appropriate CPNI safeguards
  - Unworkable – the carrier would need to unencrypt the data each time it needed to access the data
  - Once the carrier unencrypts the data (for example, for billing purposes), the data is now available in a written unencrypted format outside of the carrier's system, thus negating the benefits of encrypting the data
  - Prohibitively costly and nearly impossible for to implement an encryption system – would require complete replacement of carrier billing practices
- CPNI Breach Notification
  - FCC should not require carriers to notify customers each time a breach has occurred
  - Not all CPNI breaches result in the misuse of data
  - Puts an undue burden on carriers; carriers may not have knowledge that a breach has occurred
  - If a security breach has resulted in the breach of personally identifiable information (such as social security number or credit card number) and carriers have knowledge of the breach, then carriers already are required to notify consumers that a breach has occurred under various federal and state statutes
  - If the FCC implements a breach notification rule, then it must limit breach notification duties to when carriers have knowledge that the customer's own personal and credit information has been compromised; carriers should not be required to notify customers after each release of CPNI

The FCC Should Not Modify Carrier Obligations with Regard to Joint Venture Partners and Independent Contractors

- There is no evidence that fraudulent access to records is due to joint venture partners or independent contractors
- Modifying the rules pertaining to independent contractors and joint venture partners would have an adverse impact on carrier operations by shutting down independent sales channels
- Modifying the rules would violate the First Amendment of the U.S. Constitution

XO Supports Adoption of a Safe Harbor

- XO supports adoption of a safe harbor based on best practices
  - XO supports the following safe harbor components:
    - Carriers must develop internal written procedures to protect CPNI
    - Carriers must conduct training regarding those procedures and the protection of CPNI
    - Carriers must develop internal standards for customer authentication
    - Carriers must file CPNI certifications with the FCC annually
    - Carriers must not use social security numbers for customer authentication
  - XO does not support inclusion of the following in any safe harbor:
    - Mandatory password protection for call center inquiries
    - Optional password protection for call center inquiries, unless limited to residential accounts
    - Customer notification of unauthorized access/disclosure of CPNI

Additional Considerations

- XO supports COMPTEL's request that the FCC affirmatively prohibit language in commercial agreements that would require CLECs to relinquish their control over customer CPNI
  - Contract provisions proposed in AT&T commercial agreements interfere with a CLEC's ability to protect its customer's CPNI
  - FCC should confirm that language in AT&T's (or any other commercial agreement) that hampers a carrier's ability to protect its customers' CPNI would be deemed unenforceable
- FCC should not apply CPNI rules to ISPs or information services
  - Doing so is not supported by section 222, which applies solely to information derived from "telecommunications services"
  - Applying CPNI requirements to information services is not necessary; EPIC is concerned about the release of telephone call records, and has not demonstrated any basis for applying CPNI requirements to ISPs or information services